ABSTRACT OF THE INVENTION

A method for formation of a shared secret key using a key matrix and a corresponding authentication protocol are described. The shared secret key formation scheme is a method in which sets of secret device keys are formed from arithmetic operations on matrix keys of a key matrix. The contents of the key matrix are held in confidence by the certification authority. The selection of which matrix keys to use is based on a key selection vector assigned by the certification authority. From the secret device keys, a shared secret key may be formed in accordance with a selected authentication protocol.